UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/692,265	10/23/2003	John R. Lambert	MS1-1714US	1569

22801 7590 04/15/2009

LEE & HAYES, PLLC
601 W. RIVERSIDE AVENUE
SUITE 1400
SPOKANE, WA 99201

EXAMINER	
DUNN, DARRIN D	

ART UNIT	PAPER NUMBER
2121	

MAIL DATE	DELIVERY MODE
04/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/692,265	LAMBERT ET AL.	
	Examiner	Art Unit	
	DARRIN DUNN	2121	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 November 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,12,15-17,19-31,34-36,38,39 and 41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9, 12, 15-17, 19-31, 34-36, 38-39, and 41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The Office Action is responsive to the communication filed on 11/26/2008.

2. Claims 1-9, 12, 15-17, 19-31, 34-36, 38-39, and 41 are pending.

Claim Objections

3. Claim 39 objected to because of the following informalities: 'One of more' is recited opposed to 'one or more.' Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. 1-4, 8-9, 12, 15-17, 19-23, 27-31, 34-36, 38-39, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Clifton et al. (Developing Custom Intrusion Detection Filters

Using Data Mining, IEEE, 2000) in view over Cuppens (Managing Alerts in Multi-Intrusion Detection Environment, IEEE, 2001) and in further view over Denning (An Intrusion Detection Model, IEEE, 1987), and in further view over Vikaykumar (USPN 5745896)

7. As per claim 1, Clifton et al. teaches a method for investigating messages passed in a message-passing environment, the method comprising:

collecting message traces ([Sequential Data Mining], [Figure 2] e.g., Log (Event, FromIP, ToIP, time), i.e., message trace. A message trace is interpreted as a message generated by a machine comprising time information. The message trace further identifies the source of the message) from at least one participant (e.g., machines on a network) in the message-passing environment (e.g., network), wherein each message trace is a series of messages originating from or sent to the at least one participant ([Figure 2] e.g., it is interpreted that an attacker is represented via a machine. A machine may generate multiple attacks. The attacks are identified via Log (Event, FromIP, ToIP, time). The attacks from one machine or machines represents a series or more than a single attack. As applied to a relational database, discussed below, messages may be grouped together within the relational database forming a group or sequence), ordered by time (e.g. basic schema includes time where samples are generated over a two week period and stored in a relational database), wherein each message has a first piece describing transfer of information (e.g., Log (FromIP, ToIP)) and a second piece describing an operation being performed in the message (Log(Event));

converting identifying information ([Sequential Association Mining] e.g., basic scheme, i.e., log data, identifies machine information) pertaining to the at least one participant (e.g. machine) into an indication of a role played (e.g., attacker. A role also pertains to an intrusion attempt) by

the at least one participant in the message- passing environment (e.g. network);

assembling the messages into at least one message sequence ([SEQUENTIAL ASSOCIATION MINING], [Preliminary Results] e.g., we analyzed these logs for 2-, 3-, 4-, and 5-event sequences. A message sequence is interpreted as a grouping of messages. In one case, 2, 3, and 4-events are grouped. In another case, a relational database (discussed below) is used to store log data group together messages from a source. For example, if 20 messages are sent from sourceIP, then a relational database would be able to group these together. A message sequence (e.g., grouping) is taught in this case by grouping together 2, 3, 4, and 5-events),

wherein assembling includes combining multiple message traces (e.g., log(event, fromIP, toIP, time) into the at least one message sequence (e.g., 2,3,4, and 5-events), each message trace pertaining to one or more messages transmitted by, or received at, a participant (e.g., it is understood that a machine generates an attack, identified as an alarm. Log(event, FromIP, ToIP) is a message received, transmitted at a machine) , wherein the combining is based on one or more of, a specified participant, a specified time frame (e.g., one-minute window), a transaction nature ([Straightforward Count] e.g. Syn Flood, ident, print), and the role played by the at least one participant (e.g., FTP user);

analyzing the at least one message sequence ([Number of Occurences]) from the message-passing environment (e.g., machine based network) to extract information (e.g., count) regarding the at least one participant (e.g.. machine) in the message-passing environment

However, Clifton et al. does not teach a reference message sequence. Denning teaches a reference sequence ([VII. C. Anomaly-Record Rules] e.g., comparing observations to known patterns of events, i.e., reference sequence. It is interpreted that a pattern is a sequence of events

used to identify an abnormal or normal sequence of events. For example, two consecutive events include failed password attempts. This corresponds to a 2-event, as applied to Clifton. By comparing 2,3, and 4-events with predetermined patterns of normal 2,3,-4 events, an abnormal condition can be brought to the attention of secuirty.)

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to provide for a means to identify a normal set of events and an abnormal set of events. Clifton et al. teaches that 2,3, and 4-events that may corresponding to logged data. The events include a first command followed by a second command (e.g., 2-event). As applied to Denning, the 2-event would be observed and compared to a reference pattern (e.g., sequence) of normal/abnormal events. It is desirable to know whether a 2,3, and 4-event corresponds to an anomaly, and it would have been obvious to compare a series of events (e.g. message sequences) with a reference sequence of events (e.g., pattern of events) to ascertain event sequence anomalies. (For example, Clifton would teach a 2-event (e.g., password fail 1, password failed 2). By comparing this 2-event with a normal pattern (e.g., password fail, password successful), the first 2-event (e.g., message sequence) could be identified as abnormal)

Clifton et al., as modified, teaches a data matrix ([Sequential Association Mining] e.g., relational database where query functions are readily employed to sort, categorize, and group data within the database using keys) based on information in the at least one message sequence (Log(Event, FromIP, ToIP, time. *It is interpreted that a relational database would also enable one of ordinary skill in the art to view all messages from a single source, receiver, or event. From example, if a source sent twenty messages, all messages from that source could be grouped together using a query. In effect, this also functions as a message sequence (e.g., grouping)

However, Clifton et al. but does not teach cluster analysis is applied to the at least one message sequence. Cuppens teaches performing cluster analysis to identify and cluster alerts from data in its relational database ([4. Alert Clustering, 4.1 Similarity Relation) and forming at least one cluster based on the data matrix (e.g., relational database) ([Alert Clustering |4.1-4.2.3])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to group together similar event types (2, 3, and 4-events) to visually illustrate similar and dissimilar grouping of events. All prior art pertains to the same field of endeavor (e.g., intrusion detection), and it would have been obvious to apply clustering techniques to a data-set as an efficient and optimal means of analyzing data.

outputting the information ([Figure 2], [Section 5 - Merging Alerts and Conflict Resolution] e.g., applying cluster results)

[**Examiner note:** The claim analysis is structured to show that log data is stored in a relational database. A relational database, i.e., data matrix, enables the log data to be sorted and grouped together. The groups, whether 2-, 3-, 4-, or 5-events may be generated from the relational database using the logic used to generate the 2,3,4, and 5-event sequences. Additionally, messages from a sender and receiver may be grouped within the relational database to show all messages from the source/destination. This would represent a group or message sequence from a single participant. A similarity measure, as taught by Cuppens, shows how any grouping may be compared for the purpose of clustering. The principles of a relational database (e.g., references cites) illustrate the use of primary keys, sorting, grouping, and count functions as a way to mine data. See Vijaykumar (USPN 5745896) for applications of queries, grouping, counting, and other intended functions provided with a relational database)

8. As per claims 2 and 21, Clifton et al. teaches the method according to claim 1, wherein the message- passing environment is a network environment including plural participants coupled together via a network ([ABSTRACT])

9. As per claims 3 and 22, Clifton et al. teaches the method according to claim 2, wherein the network uses an Internet Protocol to transmit messages between participants ([Preliminary Results] e.g., FTP)

10. As per claims 4 and 23, Clifton et al. teaches the method according to claim 2, wherein the messages express the information in one of a plurality of message formats ([Preliminary Results] e.g., SYN Flood, ident, print, FTP (e.g., different formats)

11. As per claims 8 and 27, Cuppens teaches the method according to claim 1, wherein the message passing environment is a machine or system (e.g., alert based management system) including plural interacting components that function as message participants (e.. IDS modules) that function as message participants ([Figure 1] e.g., a client communicating with a central system would also include a software module (e.g., O/S, interface modules) for communicating over the network. The claim is interpreted as a network comprising a central system in communication with distributed clients, where a central system has software to collect and analyze network traffic)

12. As per claims 9 and 28, Cuppen teaches the method according to claim 1, wherein the message passing environment is a software program (e.g. alert based management system) including plural interacting software modules (e.g., IDS) that function as message participants ([Introduction], [Figure 1])

13. As per claim 12, Clifton et al. teaches the method according to claim 1, wherein the assembling comprises assembling plural message sequences (e.g., event logs are assembled into 2, 3, and 4-events), and analyzing comprises analyzing the plural message sequences (e.g., as modified, clustering is performed, supra claim 1 for pertinent citations and discussion)

14. As per claim 15, Clifton et al., as modified teaches the method according to claim 1, wherein the forming of the data matrix (e.g., relational database, supra Cuppens) involves extracting features ([Preliminary Results] e.g., Event, FromIP, ToIP) from said at least one message sequence (e.g. based on the grouping of similar messages from ToIP, a relational database counts the number of occurences), including extracting numerical counts (e.g., Count) for at least one feature present in the message sequence (e.g., counting number of messages sent from FromIP, for example), the feature including at least one of: a message command type, a sender/receiver pair (Log(FromIP, ToIP), a property of the message and an application-level property (It is interpreted that a relational database may receive event log and group (FromIP, ToIP, and Events) such that events from a sender may be classified together, events from a receiver may be classified, and the number of events may be sorted to include 2, 3,4, and 5-events)

15. As per claim 16, Cuppens teaches the method according to claim 1, wherein the forming of the data matrix involves forming a similarity measure ([Section 4. Alert Clustering] e.g., similarity function) which measures the difference between said at least one message sequence and another message sequence (e.g., when a new alert is generated, the function determines the existent of alerts in a database that can be linked. A similarity relation is defined between two alert messages. As applied to a relational database, groups of messages within the database may

be compared via applying the similarity function), wherein forming a similarity measure includes at least one of: string/sequence matching (e.g., similarity relation links Entity 1 and Entity 2) and comparing said at least one message sequence with an optimal functioning sequence, a good server trace, a bad server trace, and a known sequence from an alternate message-passing environment.

16. As per claim 17, Cuppens teaches the method according to claim 1, wherein the analyzing involves identifying results of the cluster analysis ([4.2.1- 5], [6.2] e.g., providing result to correlation function for further analysis) that may warrant further investigation, wherein the identifying includes comparing the at least one message sequence against a formal model of the message passing environment and placing the at least one message sequence into one or more clusters representing adherence to the formal model, non-adherence to the formal model and "interesting", wherein "interesting" includes indicia of beneficial phenomena, anomalous conditions, and other features which cause the at least one message sequence to be singled out from other message sequences ([4.2, 4.2.2, 4.2.3] e.g., 'at least one' of specified either selecting a) comparing a sequence against a formal model or b) interesting includes other features. Here, clustering may occur using time, source/target similarity, and classification similarity (e.g., interesting)

17. As per claims 19 and 38, Clifton et al., as modified, teaches a computer readable medium (e.g., intrusion detection system) including machine readable instructions for implementing the collecting, assembling, analyzing, and outputting recited in claim 1 (e.g. instructions, i.e., code, is implemented in Cuppens | Denning to provide pattern matching, data logging. The relational

database implements code to sort data. Cluster analysis implements code to group data based on similarity measures.

18. As per claim 20, Clifton et al., as modified, teaches an apparatus for investigating messages passed in a message-passing environment, the apparatus comprising:

message aggregation logic configured to collect a plurality of messages from at least one participant in the message-passing environment ([Sequential Associations] e.g., Log(Event, FromIp, ToIP), i.e., aggregation logic) As modified by Cuppens, a relational database is used to store the data), and to assemble the messages into at least one message sequence (e.g., 2, 3,4, and 5-events and/or using a relational database to group/sort data using attributes (From, To, Event), wherein each message has a first piece describing transfer information (e.g., From IP, ToIP) and a second piece describing an operation being performed in the message (e.g. event);

analysis logic configured ([Preliminary Results] e.g., Counts) to analyze said at least one message sequence from the message passing environment to extract information regarding at least the one participant in the message-passing environment (e.g., number of 2-event counts), wherein the analysis logic (e.g., supra claim 1, Dennings, VII.C e.g. pattern matching) is further configured to compare said at least one message sequence with a reference message sequence, the reference message sequence comprising a sequence that reflects an error-free operation in the message passing environment (e.g., supra claim 1 discussion)

cluster analysis logic (e.g., Section 4, Alert Clustering, supra Cuppens discussion, claim 1) configured to perform cluster analysis to group the at least one message sequence into at least one cluster, wherein the cluster analysis logic is configured to form a data matrix based on information in the at least one message sequence and form the at least one cluster based on the

data matrix (e.g., supra claim 1 discussion); and

output logic configured to output the information ([Figure 2])

19. As per claim 29, Clifton et al., as modified teaches the apparatus according to claim 20, wherein the message aggregation logic is further configures to convert identifying information pertaining to said at least one participant (e.g., FromIP, ToIP, Ftp User) into an indication of a role played by the participant in the message passing environment (e.g., role is not defined. A role may be an intrusion attempt, an attacker, recognizing an FTP user, etc)

20. As per claim 30, Clifton et al. as modified, teaches the apparatus according to claim 20, wherein the message aggregation logic is further configured to combine multiple message traces into said at least one message sequence (e.g., 2,3,4,5-events and/or grouping similar FromIP using a relational database), each message trace pertaining to one or more messages transmitted by and/or received at a participant (e.g., Log(Event, From, To, time)

21. As per claim 31, Clifton et al. teaches the apparatus according to claim 20, wherein the message aggregation logic is further configured to assemble plural message sequences (e.g., group together in the table, Preliminary Results), and the analysis logic is further configured to analyze the plural message sequences (e.g., Counts)

22. As per claim 34, Clifton, as modified, teaches the apparatus according to claim 20, wherein the analysis logic is configured to form the data matrix (e.g., relational database) by extracting features (e.g., (FromIP, ToIP, and/or Event) from said at least one message sequence (e.g., when a relational database is used, messages may be grouped together from the same participant, i.e., FromIP. Once grouped, messaged may be counted and/or compared to other groups from other participants)

23. As per claim 35, Clifton et al., as modified, teaches the apparatus according to claim 20, wherein the analysis logic is configured to form the data matrix by forming a similarity measure which measures the difference between said at least one message sequence and another message sequence (e.g., supra claim 16)

24. As per claim 36, Clifton et al., as modified, teaches the apparatus according to claim 20, wherein the analysis logic is further configured to identify results of the cluster analysis that may warrant further investigation (e.g., supra claim 17)

25. Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Clifton et al. (Developing Custom Intrusion Detection Filters Using Data Mining, IEEE, 2000) in view over Cuppens (Managing Alerts in Multi-Intrusion Detection Environment, IEEE, 2001) and in further view over Denning (An Intrusion Detection Model, IEEE, 1987), and in further view over Vikaykumar (USPN 5745896).

26. As per claim 39, Clifton et al. teaches a method for investigating messages passed in a message-passing environment, the method comprising:

means for collecting message traces ([Sequential Data Mining], [Figure 2] e.g., Log (Event, FromIP, ToIP, time), i.e., message trace. The means for claim terminology is interpreted as software. It is interpreted that software is used to collect the messages (e.g., Log (Event, FromIP, ToIP, and time). A message trace is interpreted as a message generated by a machine comprising time information. The message trace further identifies the source of the message) from at least one participant (e.g., machines on a network) in the message-passing environment (e.g., network), wherein each message trace is a series of messages originating from or sent to the at least one participant ([Figure 2] e.g., it is interpreted that an attacker is represented via a

machine. A machine may generate multiple attacks. The attacks are identified via Log (Event, FromIP, ToIP, time). The attacks from one machine or machines represents a series or more than a single attack. As applied to a relational database, discussed below, messages may be grouped together within the relational database forming a group or sequence), ordered by time (e.g. basic schema includes time where samples are generated over a two week period and stored in a relational database), wherein each message has a first piece describing transfer of information (e.g., Log (FromIP, ToIP)) and a second piece describing an operation being performed in the message (Log(Event));

a means for converting identifying information ([Sequential Association Mining] e.g., basic scheme, i.e., log data, identifies machine information. Software is interpreted as the 'means for' because all references utilized implement code for the collecting and data analysis) pertaining to the at least one participant (e.g. machine) into an indication of a role played (e.g., attacker. A role also pertains to an intrusion attempt) by the at least one participant in the message- passing environment (e.g. network);

means for assembling the messages into at least one message sequence ([SEQUENTIAL ASSOCIATION MINING], [Preliminary Results] e.g., software is interpreted as the 'means for'. we analyzed these logs for 2-, 3-, 4-, and 5-event sequences. A message sequence is interpreted as a grouping of messages. In one case, 2, 3, and 4-events are grouped. In another case, a relational database (discussed below) is used to store log data group together messages from a source. For example, if 20 messages are sent from sourceIP, then a relational database would be able to group these together. A message sequence (e.g., grouping) is taught in this case by grouping together 2, 3, 4, and 5-events),

wherein assembling includes combining multiple message traces (e.g., log(event, fromIP, toIP, time) into the at least one message sequence (e.g., 2,3,4, and 5-events), each message trace pertaining to one or more messages transmitted by, or received at, a participant (e.g., it is understood that a machine generates an attack, identified as an alarm. Log(event, FromIP, ToIP) is a message received, transmitted at a machine) , wherein the combining is based on one or more of, a specified participant, a specified time frame (e.g., one-minute window), a transaction nature ([Straightforward Count] e.g. Syn Flood, ident, print), and the role played by the at least one participant (e.g., FTP user);

means for analyzing the at least one message sequence ([Number of Occurences]) from the message- passing environment (e.g., machine based network) to extract information (e.g., count) regarding the at least one participant (e.g.. machine) in the message-passing environment. (the means for language is interpreted as software means. Here, clustering utilizes software code to access a relational database and subsequently perform clustering)

However, Clifton et al. does not teach a reference message sequence. Denning teaches a reference sequence ([VII. C. Anomaly-Record Rules] e.g., comparing observations to known patterns of events, i.e., reference sequence. It is interpreted that a pattern is a sequence of events used to identify an abnormal or normal sequence of events. For example, two consecutive events include failed password attempts. This corresponds to a 2-event, as applied to Clifton. By comparing 2,3, and 4-events with predetermined patterns of normal 2,3,-4 events, an abnormal condition can be brought to the attention of secuirty.)

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to provide for a means to identify a normal set of events and an abnormal set of

events. Clifton et al. teaches that 2,3, and 4-events that may corresponding to logged data. The events include a first command followed by a second command (e.g., 2-event). As applied to Denning, the 2-event would be observed and compared to a reference pattern (e.g., sequence) of normal/abnormal events. It is desirable to know whether a 2,3, and 4-event corresponds to an anomaly, and it would have been obvious to compare a series of events (e.g. message sequences) with a reference sequence of events (e.g., pattern of events) to ascertain event sequence anomalies. (For example, Clifton would teach a 2-event (e.g., password fail 1, password failed 2). By comparing this 2-event with a normal pattern (e.g., password fail, password successful), the first 2-event (e.g., message sequence) could be identified as abnormal)

Clifton et al., as modified, teaches a data matrix ([Sequential Association Mining] e.g., relational database) based on information in the at least one message sequence (Log(Event, FromIP, ToIP, time. *It is interpreted that a relational database would also enable one of ordinary skill in the art to view all messages from a single source, receiver, or event. From example, if a source sent twenty messages, all messages from that source could be grouped together. In effect, this also functions as a message sequence (e.g., grouping) but does not teach cluster analysis applied to the at least one message sequence. Cuppens teaches performing cluster analysis to identify and cluster alerts from data in its relational database ([4. Alert Clustering, 4.1 Similarity Relation) and forming at least one cluster based on the data matrix (e.g., relational database) ([Alert Clustering |4.1-4.2.3])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to group together similar event types (2, 3, and 4-events) to visually illustrate similar and dissimilar grouping of events. All prior art pertains to the same field of endeavor (e.g.,

intrusion detection), and it would have been obvious to apply clustering techniques to a data-set as an efficient and optimal means of analyzing data.

means for storing the at least one message sequence in a master collection of message sequences (e.g., relational database, supra Cuppens Introduction. A relational database stores any message grouping)

means for culling the master collection of message sequences for at least one subset of a message sequence based on specified criteria including one of more of: a specified time range, transaction type, participants involved in at least one message exchange, objectives of an analyst and a nature of the messaqe- passing environment involved (e.g., a relational database enables data to be sorted via time, which in view over Clifton, i.e., time analysis, enables a certain sub-subset of messages to be localized. The From and To participants may be grouped according to time, similar events, etc using a relational database, etc); and

means for storing the at least one subset for subsequent analysis (e.g., relational database, i.e., means for storing);

means for outputting the information ([Figure 2], [Section 5 - Merging Alerts and Conflict Resolution] e.g., applying cluster results. Software is interpreted as the means)

27. As per claim 41, Clifton et al., as modified, teaches the apparatus according to claim 20, wherein the reference message sequence is a sequence that reflects known failure conditions within the message passing environment (e.g., supra claim 1 discussion)

28. Claims 5-7 & 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Clifton et al. (Developing Custom Intrusion Detection Filters Using Data Mining, IEEE, 2000) in view over Cuppens (Managing Alerts in Multi-Intrusion Detection Environment, IEEE, 2001)

and in further view over Denning (An Intrusion Detection Model, IEEE, 1987), and in further view over Greifeneder et al. (USPN 20040243349)

29. As per claims 5 and 24, Clifton et al., as modified, teaches a analyzing network traffic for events but does not teach where the messages include information expressed in a markup language. Greifeneder et al teaches that network traffic may comprise documents including XML, GIF, and JPG communicated using network protocols, including but not limited to SOAP ([0064], [0019])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Clifton et al. to include xml based messages. Scarfe et al. teaches collecting information pertaining to network traffic for classification and analysis. Greifeneder et al. teaches a method and system for monitoring and the analysis of networked systems. Xml based messages are a common format utilized in network communication. Since xml messages include data about data, it would have been obvious to group and analyze such messages for pertinent information about the behavior of a sender/receiver within a network.

34. As per claims 6 and 25, Greifeneder et al. teaches wherein the markup language is xml ([0064] e.g. XML)

35. As per claims 7 and 26, Greifeneder et al. teaches wherein the network uses Simple Object Access Protocol to transmit messages between participants ([0019] e.g. SOAP)

Response to Amendment

30. The amendment filed, 11/26/2008, has been considered and made of record.

Response to Arguments

31. Applicant's arguments with respect to claims 1-9, 12, 15-17, 19-31, 34-36, 38-39, and 41 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

32. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

20040186826 – real time aggregation of data for SQL

20040143749 – intrusion detection

20030236652 – anomaly detection

7162464 – data mining in a relational database

7150044 – anomalous event detection system

6615205 – clustering

5721910 – grouping together similar categories together

5675784 – using relational database to search for components

33. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARRIN DUNN whose telephone number is (571)270-1645. The examiner can normally be reached on EST:M-R(8:00-5:00) 9/5/4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert DeCady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. D./ Ramesh Patel

Examiner, Art Unit 2121
04/10/09

Primary Examiner
Art Unit 2121

/Ramesh B. Patel/

Primary Examiner, Art Unit 2121